PTO/SB/08a (08-03 )
Approved for use through 07/31/2006. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

| INFORMATION DISCLOSURE STATEMENT BY APPLICANT ( Not for submission under 37 CFR 1.99) | Application Number | 10626420 |
| --- | --- | --- |
| | Filing Date | 2003-07-24 |
| | First Named Inventor | Sheueling Chang Shantz |
| | Art Unit | 2436 |
| | Examiner Name | Johnson, Carlton |
| | Attorney Docket  Number | 6000-32301 |

| U.S.PATENTS | | | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| Examiner Initial* | Cite No | Patent Number | Kind Code1 | Issue Date | Name of Patentee or Applicant of cited Document | Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear |
| /CJ/ | 1 | 5347481 | | | Lambert, et al. | |
| | 2 | 6049815 | | | Lambert, et al. | |
| | 3 | 6199087 | | | Blake, et al. | |
| | 4 | 6763365 | | | Chen, et al. | |
| | 5 | 4863247 | | | Lasher, et al. | |
| | 6 | 6687725 | | | Chen, et al. | |
| | 7 | 7240084 | | | Gura, et al. | |
| | 8 | 7346159 | | 2008-03-18 | Gura, et al. | |

| | | | | | |
|---|---|---|---|---|---|
| INFORMATION DISCLOSURE STATEMENT BY APPLICANT ( Not for submission under 37 CFR 1.99) | | Application Number | 10626420 | | |
| | | Filing Date | 2003-07-24 | | |
| | | First Named Inventor | Sheueling Chang Shantz | | |
| | | Art Unit | 2436 | | |
| | | Examiner Name | Johnson, Carlton | | |
| | | Attorney Docket Number | 6000-32301 | | |

| | | | | | |
|---|---|---|---|---|---|
| /CJ/ | 9 | 7461115 | | 2008-12-02 | Eberle, et al. |

If you wish to add additional U.S. Patent citation information please click the Add button.

## U.S.PATENT APPLICATION PUBLICATIONS

| Examiner Initial* | Cite No | Publication Number | Kind Code[1] | Publication Date | Name of Patentee or Applicant of cited Document | Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear |
|---|---|---|---|---|---|---|
| /CJ/ | 1 | 20030123654 | | | Lambert, et al. | |
| | 2 | 20030123655 | | | Lambert, et al. | |
| | 3 | 20020044649 | | | Gallant, et al. | |
| | 4 | 20040158597 | | | Ye, et al. | |

If you wish to add additional U.S. Published Application citation information please click the Add button.

## FOREIGN PATENT DOCUMENTS

| Examiner Initial* | Cite No | Foreign Document Number[3] | Country Code[2] i | Kind Code[4] | Publication Date | Name of Patentee or Applicant of cited Document | Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear | T[5] |
|---|---|---|---|---|---|---|---|---|
| | 1 | | | | | | | ☐ |

If you wish to add additional Foreign Patent Document citation information please click the Add button

## NON-PATENT LITERATURE DOCUMENTS

| Examiner Initials* | Cite No | Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published. | T[5] |
|---|---|---|---|

| | | | | |
|---|---|---|---|---|
| INFORMATION DISCLOSURE STATEMENT BY APPLICANT ( Not for submission under 37 CFR 1.99) | | Application Number | 10626420 | |
| | | Filing Date | 2003-07-24 | |
| | | First Named Inventor | Sheueling Chang Shantz | |
| | | Art Unit | 2436 | |
| | | Examiner Name | Johnson, Carlton | |
| | | Attorney Docket Number | 6000-32301 | |

| /CJ/ | 1 | U.S. Application Serial No. 11/625,659 filed 1/22/07. | ☐ |
|---|---|---|---|
| | 2 | U.S. Application Serial No. 10/789,311 filed 2/27/04. | ☐ |
| | 3 | U.S. Application Serial No. 12/256,295 filed 10/22/08. | ☐ |
| | 4 | U.S. Application Serial No. 10/387,007 filed 3/11/03. | ☐ |
| | 5 | U.S. Application Serial No. 10/996,103 filed 11/23/04. | ☐ |
| | 6 | ERDEM, et al., "A Less Recursive Variant of Karatsuba-Ofman Algorithm for Multiplying Operands of Size a Power of Two," Proceedings of the 16th IEEE Symposium on Computer Arithmetic (ARITH-16'03), June 15-18, 2003. | ☐ |
| | 7 | Gupta, V., et al, "Speeding up Secure Web Transactions Using Elliptic Curve Cryptography," Sun Microsystems, Inc., http://research.sun.com/projects/crypto/, 9 pages. | ☐ |
| | 8 | Comba, P.G., "Exponentiation Cryptosystems on the IBM PC," IBM Systems Journal, Vol. 29, No. 4, 1990, pp. 526-538. | ☐ |
| | 9 | Kaliski, Burt, "TWIRL and RSA Key Size," Technical Notes, May 1, 2003, RSA Laboratories, 5 pages, downloaded from Internet http://www.orsasecurity.com/rsalabs/node.asp?id=2004 as of September 13, 2006. | ☐ |
| | 10 | Gura, Nils, et al., "Comparing Elliptic Curve Cryptographic and RSA on 8-bit CPUs," Cryptographic Hardware and Embedded Systems – CHES 2004: 6th International Workshop (Cambridge, MA, USA), August 11-13, 2004, LNCS, Vol. 3156, ISBN 3-540-22666-4, pp. 119-132, Springer. | ☐ |
| | 11 | Karatsuba, A., et al., "Ymnozhenie mnogozhachnix chisel na avtomatax," Doklady Academi Nauk SSSR, Vo. 145. No. 2, pp. 293-294, 1962. | ☐ |

| | | | |
|---|---|---|---|
| INFORMATION DISCLOSURE STATEMENT BY APPLICANT ( Not for submission under 37 CFR 1.99) | Application Number | 10626420 | |
| | Filing Date | 2003-07-24 | |
| | First Named Inventor | Sheueling Chang Shantz | |
| | Art Unit | 2436 | |
| | Examiner Name | Johnson, Carlton | |
| | Attorney Docket Number | 6000-32301 | |

| | | | |
|---|---|---|---|
| /CJ/ | 12 | Hankerson, et al., "Guide to Elliptic Curve Cryptography," pp. 48-53, 95-113, 129-147, 205-212 and 224-226, Springer-Verlag, 2004. | ☐ |
| | 13 | Cohn, Leonard Allen, "Generate-Propogate Adders," ChoPP Computer Corporation, prior 2000, pp. 1-16. | ☐ |
| | 14 | Mano, M. Morris, "Computer System Architecture," Prentice-Hall, Inc., 1976, pp. 244-249. | ☐ |
| | 15 | Guajardo, et al., "Efficient Algorithms for Elliptic Curve Cryptosystems," ECE Dept., Worcester Polytechnic Institute, pp. 1-16 (CRYPTO '97, Springer-Verlag, LNCS 1294, pp. 342-356, 1997). | ☐ |
| | 16 | Weimerskirch, et al., "Generalizations of the Karatsuba Algoirthm for Polynomial Multiplication," Communication Security Group, Dept. of Electrical Engineering & Information Sciences, Ruhr-Universitat, Germany, March 2002, pp. 1-23. | ☐ |
| | 17 | Blake-Wilson, S., "Additional ECC Groups for IKE", IPSec Blake-Wilson, Dierks, Hawk-Working Group, July 23, 2002, pp. 1-17. | ☐ |
| | 18 | Gupta, V., "ECC Cipher Suites for TLS," Blake-Wilson, Dierks, Hawk – TLS Working Group, August 2002, pp. 1-31. | ☐ |
| | 19 | "RFC 2246 on the TLS Protocol Version 1.0", http://www.ietf.org/mail-archive/ietf-announce/Current/msg02896.html, March 26, 2003, 2 pages, including Dierks, T., "The TLS Protocol Version 1.0", Dierks & Allen, January 1999, pp. 1-80. | ☐ |
| | 20 | Song, et al., "Low-Energy Digit-Serial/Parallel Finite Field Multipliers," Journal of VLSI Signal Processing 19, 1988, pp. 149-166. | ☐ |
| | 21 | Agnew, et al., "An Implementaion of Elliptic Curve Cryptosystems Over F2155," IEEE Journal on Selected Areas on Communications, Vol. 11. No. 5, June1993, pp. 804-813. | ☐ |
| | 22 | Halbutogullari, et al., "Mastrovito Multiplier for General Irreducible Polynomials," IEEE Transactions on Computers, Vo. 49, No. 5, May 2000, pp. 503-518. | ☐ |

| | | | |
|---|---|---|---|
| INFORMATION DISCLOSURE STATEMENT BY APPLICANT ( Not for submission under 37 CFR 1.99) | Application Number | 10626420 | |
| | Filing Date | 2003-07-24 | |
| | First Named Inventor | Sheueling Chang Shantz | |
| | Art Unit | 2436 | |
| | Examiner Name | Johnson, Carlton | |
| | Attorney Docket  Number | 6000-32301 | |

| /CJ/ | 23 | Yanik, et al., "Incomplete Reduction in Modular Arithmetic," IEEE Proc.-Comput. Digit. Tech., Vol. 149, No. 2, March 2002, pp. 46-52. | ☐ |
|---|---|---|---|
| | 24 | Blum, et al., "High-Radix Montgomery Modular Exponentiation on Reconfigurable Hardware," IEEE Transactions on Computers, Vol. 50, No. 7, July 2001, pp. 759-764. | ☐ |
| | 25 | Orlando, et al., August 2000, "A High-Performance Reconfigurable Elliptic Curve Processor for GF(2m)," CHES 2000 Workshop on Cryptographic Hardware and Embedded Systems, Springer-Verlag, Lecture Notes in Computer Science, 1965, pp. 41-56. | ☐ |
| | 26 | Lopez, et al., August 1999, "Fast Multiplication on Elliptic Curves over GF(2m) without Precomputation," CHES 1999 Workshop on Cryptographic Hardware and Embedded Systems, Springer-Verlag, Lecture Notes in Computer Science, 1717, pp. 316-327. | ☐ |
| | 27 | Hankerson, et al., August 2000, "Software Implementation of Elliptic Curve Cryptography over Binary Fields," CHES 2000 Workshop on Cryptographic Hardware and Embedded Systems, Springer-Verlag, Lecture Notes in Computer Science, 1965, pp. 1-24. | ☐ |
| | 28 | Koblitz, Neal, "Elliptic Curve Cryptosystems," Mathematics of Computation, Vo. 48, NO. 177, January 1987, pp. 203-209. | ☐ |
| | 29 | Schroeppel, et al., 1995, "Fast Key Exchange with Elliptic Curve Systems," Advances in Cryptography, Crypto '95, Springer-Verlag, Lecture Notes in Computer Science 963, pp. 43-56. | ☐ |
| | 30 | Gao, et al., "A Compact Fast Variable Key Size Elliptic Curve Cryptosystem Coprocessor," Proceedings of the Seventh Annual IEEE Symposium on Field-Programmable Custom Computer Machines, 1998. | ☐ |
| | 31 | Miller, V., "Use of Elliptic Curves of Cryptography," In Lecture Notes in Computer Science 218, Advances in Cryptology, CRYPTO '85, pp. 417-426, Springer-Verlag, Berling, 1986. | ☐ |
| | 32 | Itoh, et al., "A Fast Algorithm for Computer Multiplicative Inverses in GF(2m) Using Normal Bases," Informaiton and Computation, Vol. 78, NO. 3, 1988, pp. 171-177. | ☐ |
| | 33 | Bednara, et al., "Reconfigurable Implementation of Elliptic Curve Crypto Algorithms," Proceedings of the International Parallel and Distributed Processing Symposium, IEEE Computer Society, 2002, 8 pages. | ☐ |

| | | | | |
|---|---|---|---|---|
| INFORMATION DISCLOSURE STATEMENT BY APPLICANT ( Not for submission under 37 CFR 1.99) | | Application Number | 10626420 | |
| | | Filing Date | 2003-07-24 | |
| | | First Named Inventor | Sheueling Chang Shantz | |
| | | Art Unit | 2436 | |
| | | Examiner Name | Johnson, Carlton | |
| | | Attorney Docket Number | 6000-32301 | |

| | | | |
|---|---|---|---|
| /CJ/ | 34 | U.S. Dept. of Commerce/National Institute of Standards and Technology, "Digital Signature Standard (DSS)," Federal Information Processing Standards Publication, January 27, 2000, pp. 1-74. | ☐ |
| | 35 | Blake-Wilson, et al, "ECC Cipher Suites for TLS," Blake-Wilson, Dierks, Hawk—TLS Working Group, March 15, 2001, pp. 1-22. | ☐ |
| | 36 | Goodman, et al., "An Energy-Efficient Reconfigurable Public-Key Cryptography Processor," IEEE Journal of Solid-State Circuits, Vol. 36, No. 11, November 2001, pp. 1808-1820. | ☐ |
| | 37 | Ernst, et al., "Rapid Prototyping for Hardware Accelerated Elliptic Curve Public-Key Cryptosystems," 12th IEEE Workshop on Rapid System Prototyping, Monterey, CA June 2001, pp. 24-29. | ☐ |
| | 38 | Blake, et al., "Elliptic Curves in Cryptography," London Mathematical Society Lecture Note Series 265, Cambridge University Press, UK, 1999, pp. vii-204. | ☐ |

If you wish to add additional non-patent literature document citation information please click the Add button

**EXAMINER SIGNATURE**

| Examiner Signature | /Carlton Johnson/ | Date Considered | 06/17/2009 |
|---|---|---|---|

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

[1] See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. [2] Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). [3] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [4] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [5] Applicant is to place a check mark here if English language translation is attached.